The opinion in support of the decision being entered today is *not*
binding precedent of the Board

UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

_____

Ex parte GARY L. GRAUNKE,
MICHAEL S. RIPLEY, and ERNIE BRICKELL

_____

Appeal 2007-0463
Application 09/896,537
Technology Center 2100

_____

Decided: August 2, 2007

_____

Before JOHN C. MARTIN, LANCE LEONARD BARRY, and
MAHSHID D. SAADAT, *Administrative Patent Judges.*

MARTIN, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal from the Examiner's August 1, 2005, rejections of claims 1-
22, all of the pending claims, under 35 U.S.C. § 102(b) or § 103(a) (Final Action 3,
5).[1] We have jurisdiction under 35 U.S.C. §§ 6(b) and 134(a). We affirm.

_____

[1] Appellants' amended Brief, filed April 25, 2006, incorrectly identifies the
(Continued on next page.)

Inasmuch as claims 4-10 and 17-19 were canceled by the Amendment After Final filed February 1, 2006, which was approved for entry in the April 11, 2006, Advisory Action, the appeal is dismissed as to those claims.

Appellants' invention relates to digital rights management and more particularly to the hierarchical protection of digital content (Specification 2, para. 0002). Content may have one or more attributes, such as resolution, frame rate, number of copies, number of simultaneous users, or size of computer (*id.* at 2, para. 0004). For instance, video content may comprise the attributes of resolution and frame rate (*id.*).

The invention permits the content to be encrypted once and distributed to multiple environments having various levels of security (*id.* at 5, para. 0014). The invention provides multi-level and multi-dimensional encoding. Multi-dimensional encoding refers to encoding content that may have one or more attributes, such as resolution or frame-rate (*id.* at 5, para. 0015). Multi-level encoding refers to hierarchical encoding of content for a given attribute (*id.*).

Multi-dimensional content is divided into sections (*id.* at 5, para. 0016). Each section is a portion of the content to be distributed and is separately encrypted using a separate key from a hierarchy of keys (*id.*). In the example depicted in Figure 1 (reproduced below), content 100 having three attributes (corresponding to dimensions 124) is transformed into encrypted content 102 comprising a plurality

---

rejected claims as claims 1-28 and incorrectly gives the date of the rejection as October 7, 2007 (Br. 2, para. III).

of encrypted sections 104, 106, 108, 110, 112, where each section corresponds to one of L through N levels of access (L<N), with L being the lowest level of access (e.g., lowest resolution) and N being the highest level of access (e.g., highest resolution) (*id.* at 6-7, para. 0021). That is, sections 104, 106, 108, 110, 112 are encrypted using respective different keys 114 (K_1), 116 (K_2), 118 (K_3), 120 (K_4), and 122 (K_5), of which key K_5 represents the highest level of access.
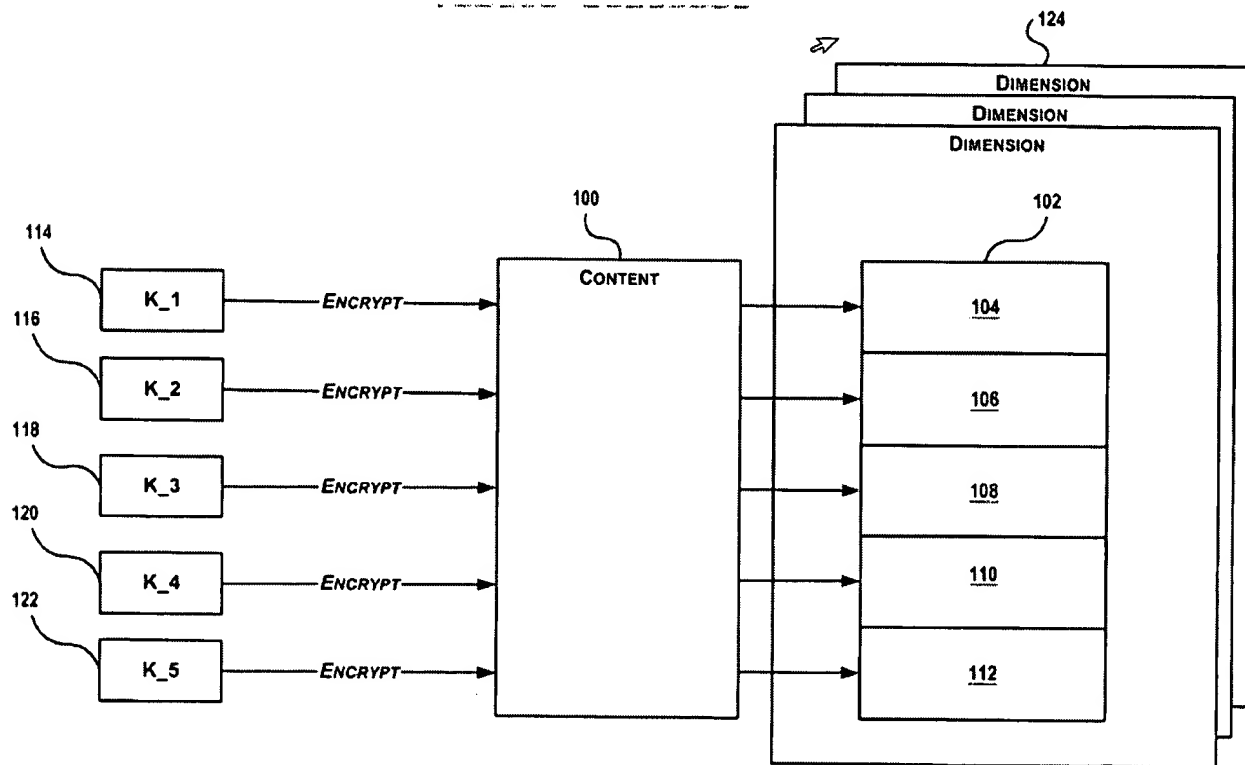

FIG. 1

As illustrated in Figure 2 (reproduced below), a server 200 and a client 202 create a secure authenticated channel 204 that connects a digital rights management

agent 208 (hereinafter "agent") of the client with a content clearinghouse 206

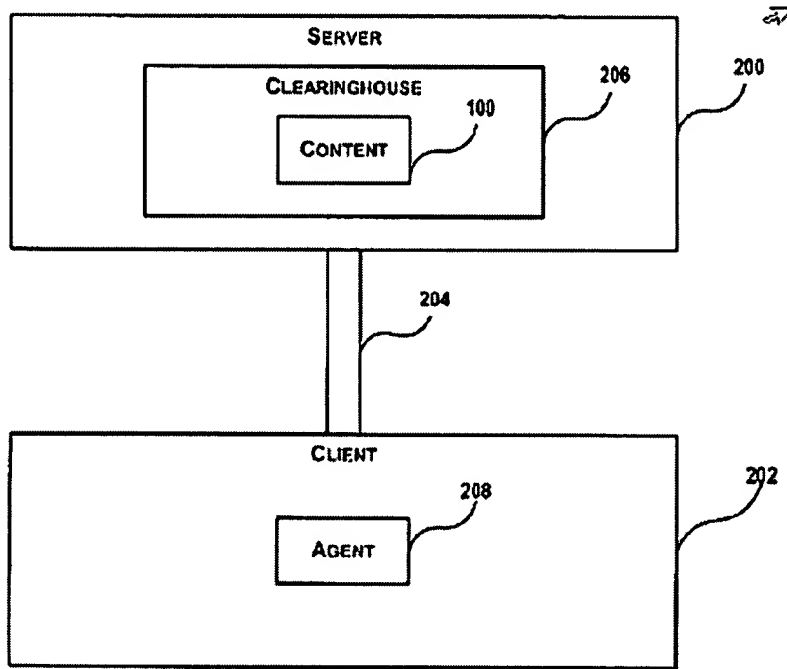comprising content 100 on the server 200 (*id.* at 7, para. 0023). A request to access

FIG. 2

content 100 is received from the client 202 (*id.*). When the server 200 receives

appropriate payment from the client 202 for an M (L<=M<=N) level of access, the

encrypted content 102 is communicated to the client 202, along with the appropriate

key for the level of access subscribed to (*id.*).

In preferred embodiments, the keys are related by a cryptographic-strength

one-way function (*id.* at 5, para. 0016). This permits the agent 208 in the client 202

to derive lower keys from the "base key" that corresponds to the client's authorized

access level. Referring to the example depicted in FIG. 3 (reproduced below),

using base key 300 (i.e., the key commensurate with the client's subscription, or

rights, which is K_3 in this example), the agent 208 can create all of the appropriate

lower level keys (302 and 304 in this example) (*id.* at 7, para. 0024). Once all

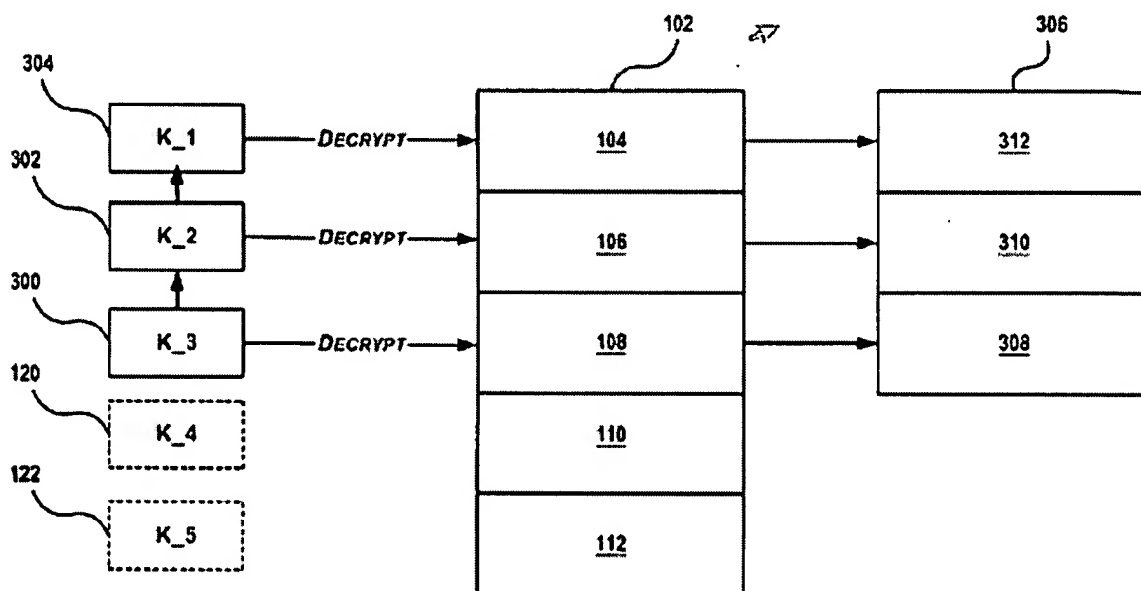appropriate keys 300, 302, 304 have been obtained or created, the encrypted

FIG. 3

content 102 is decrypted into accessible content 306, i.e., sections 308, 310, and

312 of the content 100 (*id.*).

THE CLAIMS

The independent claims before us are claims 1, 11, 14, and 20, of which claim 1 reads:

> 1. A method comprising:
>
> receiving content comprising a set of attributes having L through N levels of access, where L<N, and content at a given level of access being decryptable by a corresponding key;
>
> receiving a base key corresponding to an M of N level of access, where L<=M<=N; and
>
> deriving lower level keys based on the base key, the lower level keys being used to access content having an M level of access or lower.

The other independent claims recite similar limitations.

THE REFERENCES AND REJECTIONS

The Examiner relies on the following references:

Arazi	US 5,448,639	Sep. 5, 1995
Eyer	US 5,485,577	Jan. 16, 1996

Claims 1, 2, 11, 12, 14, 15, 20, and 21 stand rejected under 35 U.S.C. § 102(b) for anticipation by Eyer.

Claims 3, 13, 16, and 22 stand rejected under § 103(a) for obviousness over Eyer in view of Arazi.

Because Appellants argue the claims rejected for anticipation as a group, we will consider only claim 1 as to that ground of rejection. 37 C.F.R.

§ 41.37(c)(1)(vii) (2005).[2] Similarly, because the claims rejected for obviousness are argued as a group, we will consider only claim 3 as to that ground of rejection. *Id.*

THE ISSUES[3]

1. Does Eyer disclose content comprising a set of attributes having L through N levels of access, as recited in claim 1?

2. Has the Examiner established that the subject matter of claim 3 would have been obvious over Eyer in view of Arazi?

PRINCIPLES OF LAW REGARDING ANTICIPATION

Application claims are interpreted as broadly as is reasonable and consistent with the specification, "taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in

---

[2] The brief was filed in April 2006.

[3] The issues as stated herein represent the contentions of Appellants, who have the burden on appeal to the Board to point out the errors in the Examiner's position. *See Gechter v. Davidson*, 116 F.3d 1454, 1460, 43 USPQ2d 1030, 1035 (Fed. Cir. 1997) ("[W]e expect that the Board's anticipation analysis be conducted on a limitation by limitation basis, with specific fact findings for each *contested* limitation and satisfactory explanations for such findings.") (emphasis added); *In re Rouffet*, 149 F.3d 1350, 1355, 47 USPQ2d 1453, 1455 (Fed. Cir. 1998) ("On appeal to the Board, an applicant can overcome a rejection [for obviousness] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.").

the applicant's specification." *In re Morris*, 127 F.3d 1048, 1054, 44 USPQ2d 1023, 1027 (Fed. Cir. 1997).

Anticipation is a question of fact. *In re Schreiber*, 128 F.3d 1473, 1477, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997). "To anticipate a claim, a prior art reference must disclose every limitation of the claimed invention, either explicitly or inherently." (*Id.*)

DISCUSSION OF ANTICIPATION REJECTION

Eyer's disclosure relates generally to security apparatus for information processing systems and is particularly useful in connection with the secure transmission of premium television services via satellite or cable (col. 1, ll. 7-13). Typically, a system subscriber is provided with a decoder connected between a television signal source (e.g., cable feed or satellite receiver) and a television set (col. 1, ll. 18-21). Each subscriber's decoder is remotely accessed by the system operator to enable or disable the receipt of specific services such as the Home Box Office (HBO) movie channel or special pay-per-view sports events (col. 1, ll. 21-25).

Eyer explains that an example of a prior art communication system using encrypted category keys and program keys is the VideoCipher® II+ scrambling system produced and licensed by General Instrument Corporation of San Diego, California, to provide encrypted satellite television communication (col. 1, ll. 49-53). The encrypted category key is derived from a category key, a unit key specific to a subscriber decoder, and access rights defining which services the particular

subscriber is entitled to receive (col. 1, ll. 53-57). The access rights are

authenticated in the category key (col. 1, ll. 57-58). A problem with this and other

known systems is that it has been necessary to provide the authenticated access

rights with the encrypted category key in a single "category rekey" message (col. 1,

ll. 59-62). However, the access rights may be many bytes in length and each

category rekey message has a limited length (col. 1, ll. 62-65). If the number of

bytes required to define access rights were to become too large, a single category

rekey message could not hold the full description (col. 1, l. 67 to col. 2, l. 3).

Eyer discloses an access control system in which access rights can be

delivered incrementally to an access control processor using more than one category

rekey message (col. 2, ll. 4-6 and 19-21). More particularly,

> [d]ata defining the access rights is divided into a plurality of
> subgroups. The subgroups are transmitted to the processor as
> authenticated data in a plurality of messages. A current cryptographic
> key is derived using the authenticated data contained in a current
> message upon receipt of that message by the processor. Each of the
> subgroups is stored in a corresponding storage bank of the processor.
> Each of the storage banks has a validity designation associated
> therewith for said cryptographic key.

(Col. 2, ll. 19-24.)

Figure 2 of Eyer shows a key hierarchy that can be used for key encryption

(col. 4, ll. 48-49).

The only limitation of claim 1 argued by Appellants in response to the

anticipation rejection is the step of "receiving content comprising a set of attributes

having L through N levels of access" (Br. 17). We understand the phrase "a set of

9

attributes" to mean a plurality of attributes. As a result, the phrase "a set of

attributes having L through N levels of access" is broad enough to read on plurality

of attributes having respective levels of access L through N. Thus, the claim does

not require that each attribute have access levels L through N.

In the Final Action, the Examiner read the recited "L through N levels of

access" on Eyer as follows:

> Eyer discloses that the television signals have subscription and
> premium services (Col. 1, lines 14-30), which would correspond to the
> different levels of access. For example[,] the base level of access
> would be your run of the mill basic cable, and the maximum level of
> access, which corresponds to N of the claims, would be access to all
> channels that the television provider has available. Element M of the
> claims would correspond to some point in between, which could be
> basic cable plus HBO for example. These levels of access are
> represented in the access rights that the terminals receive and
> furthermore in the decryption keys that are later generated from those
> access rights. Therefore Eyer discloses the "levels of access" as
> claimed.

(Final Action 2.) Appellants' sole argument in response to the rejection is that

> [t]he claims of the subject application clearly require receiving
> "content comprising a set of _attributes having L through N levels of_
> _access_" (emphasis added). While Eyer discloses data that may be
> divided into a plurality of subgroups, Eyer does not disclose that such
> data has attributes which have levels of access as required by the
> claimed invention.

(Br. 17.) In the Answer, the Examiner responded by more particularly explaining

that:

> Eyer discloses a method of controlling access to video data using
> various access rights. This video data contains different types of video

> data in the form of premium services such as HBO or special pay-per-view services, and of course standard channels (Col. 1, lines 14-25 & Col. 4, lines 48-63). . . . In applying the Eyer reference, one would recognize that video data is divided into channels that are categorized as standard/premium/pay-per-view channels. . . . Therefore, each channel of the video data in Eyer would be considered a section of the content that represents a level of access for the attributes of the content as described in the [i.e., Appellants'] specification.

(Answer 4-5.) It is therefore clear that the Examiner is reading the recited "content comprising a set of attributes having L through N levels of access" collectively on the standard, premium, and pay-per-view video channels, with the result that the recited "set of attributes" corresponds to the set of designations of the channels as standard, premium, or pay-per-view. This position strikes us as a sound one. Appellants' above-quoted sole argument from the Brief (at 17) is not responsive to the rejection, because the argument incorrectly presumes that the Examiner is reading the recited "content comprising a set of attributes having L through N levels of access" on the subgroups of data that are used to define the access rights. Nor have Appellants filed a Reply Brief pointing out any error in the Examiner's position.

We are therefore affirming the § 102(b) rejection as to claim 1 and also as to claims 2, 11, 12, 14, 15, 20, and 21, which are not separately argued. 37 C.F.R. § 41.37(c)(1)(vii) (2005).

PRINCIPLES OF LAW REGARDING OBVIOUSNESS

A rejection under 35 U.S.C. § 103(a) must be based on the following factual determinations: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) objective indicia of non-obviousness. *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360, 80 USPQ2d 1641, 1645 (Fed. Cir. 2006) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (1966)).

"The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Leapfrog Enter., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161, 82 USPQ2d 1687, 1691 (Fed. Cir. 2007) (quoting *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1739-40, 82 USPQ2d 1385, 1395 (2007)). "One of the ways in which a patent's subject matter can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *KSR*, 127 S. Ct. at 1742, 82 USPQ2d at 1397.

Discussing the obviousness of claimed combinations of elements of prior art, *KSR* explains:

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is

> obvious unless its actual application is beyond his or her skill.
> *Sakraida* [*v. AG Pro, Inc.,* 425 U.S. 273, 189 USPQ 449 (1976)] and
> *Anderson's-Black Rock*[*, Inc. v. Pavement Salvage Co.,* 396 U.S. 57,
> 163 USPQ 673 (1969)] are illustrative—a court must ask whether the
> improvement is more than the predictable use of prior art elements
> according to their established functions.

KSR, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot

be fairly characterized as involving the simple substitution of one known element

for another or the mere application of a known technique to a piece of prior art

ready for the improvement, a holding of obviousness can be based on a showing

that there was "an apparent reason to combine the known elements in the fashion

claimed." *KSR,* 127 S. Ct. at 1740-41, 82 USPQ2d at 1396. In other words, "there

must be some articulated reasoning with some rational underpinning to support the

legal conclusion of obviousness." *Id.,* 127 S. Ct. at 1741, 82 USPQ2d at 1396

(quoting *In re Kahn,* 441 F.3d 977, 987, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)).

However, this reasoning is not limited to the problem the patentee was trying to

solve; "*any* need or problem known in the field of endeavor at the time of invention

and addressed by the patent can provide a reason for combining the elements in the

manner claimed," *KSR,* 127 S. Ct. at 1742, 82 USPQ2d at 1397 (emphasis added).

The reasoning given as support for a conclusion of obviousness can be based

on interrelated teachings of multiple patents, the effects of demands known to the

design community or present in the marketplace, and the background knowledge

possessed by a person having ordinary skill in the art. *KSR,* 127 S. Ct. at 1740-41,

82 USPQ2d at 1396. *See also Leapfrog,* 485 F.3d at 1162, 157 82 USPQ2d at 1691

(holding it "obvious to combine the Bevan device with the SSR to update it using

modern electronic components in order to gain the commonly understood benefits of such adaptation, such as decreased size, increased reliability, simplified operation, and reduced cost").

Furthermore, a reference may be understood by the artisan as suggesting a solution to a problem that the reference does not discuss. *See KSR*, 137 S. Ct. at 1742, 82 USPQ2d at 1397 ("Common sense teaches . . . that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle. . . . A person of ordinary skill is also a person of ordinary creativity, not an automaton.").

ANALYSIS OF THE OBVIOUSNESS REJECTION

Claim 3 reads:

> 3. The method of claim 1, wherein said deriving lower keys based on the base key comprises, for a given lower level key, using a modular exponentiation of a higher level key.

Eyer does not disclose that the key process uses modular exponentiation. For this teaching, the Examiner relies on Arazi, which relates to devices for applying digital signatures, to hardware for performing modular arithmetic operations that form the basis of modern cryptography, and to methods for performing cryptographic operations such as are carried out in the operation of digital signature devices (DSDs) (col. 1, ll. 5-10). Arazi's DSD comprises hardware or software means for carrying out modular exponentiation and/or modular multiplication operations (col. 1, ll. 47-50). The Examiner (Answer 4) characterizes Arazi's

specification at column 11, lines 30-38 as disclosing RSA key generation using

modular exponentiation methods. Appellants do not dispute this characterization.

As motivation for modifying Eyer to employ modular exponentiation, the

Examiner (Final Action 5) cites the reduction in overhead mentioned in the

following passage in Arazi:

> The major contribution of this method is due to the fact that the
> NIST-DSS publication (Federal Register, Aug. 30 1991, pp. 42919-
> 43546, indicate the usage of the Euclid algorithm, involving division
> operations, and a dedicated control program. The present method
> avoids this overhead, calculating the modular multiplicative inverse
> modulo q by using the already available modular exponentiator, which
> forms an integral part of the DSS circuitry.

(Arazi, col. 11, ll. 58-66).

> Appellants responded to the obviousness rejection by arguing that:

> [t]he fact that Eyer may use digital signatures . . . does not make it a
> candidate for combination with Arazi absent a suggestion for
> desirability of the combination. Applicants submit that such
> suggestion is absent because the references address different needs.
> Eyer addresses a need for a secure method for transmission of data,
> while Arazi addresses a need for a simplified and less expensive digital
> signature device. Applicants respectfully submit that the combination
> of Eyer with Arazi is not suggested in either reference.

(Br. 19). This argument is unconvincing because it fails to take into account that a

reference may be understood by the artisan as suggesting a solution to a problem

that the reference does not discuss. *Id.*, 127 S. Ct. at 1742, 82 USPQ2d at 1397

("Common sense teaches . . . that familiar items may have obvious uses beyond

their primary purposes, and in many cases a person of ordinary skill will be able to

fit the teachings of multiple patents together like pieces of a puzzle. . . . A person of ordinary skill is also a person of ordinary creativity, not an automaton.").

Appellants have not pointed out any error in the Examiner's rationale that the artisan would have been motivated to combine the teachings of Eyer and Arazi in order to reduce overhead. Instead, after quoting (Br. 19-20) the Examiner's rationale, they cite *Ex parte Clapp*, 227 USPQ 972, 973 (BPAI 1985) for the proposition that the Examiner bears the burden of "present[ing] a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teaching of the references" (Br. 20) and then simply assert "that the Examiner has failed to meet this burden, and maintain that both Eyer and Arazi lack the suggestion or motivation for combination" (*id.*).

Finally, Appellants argue that Eyer does not disclose "content comprising a set of attributes having L through N levels of access," as required by claim 1, and that Arazi does not cure this defect (*id.*). This argument is unconvincing for the reasons given above in the discussion of the anticipation rejection.

Because Appellants have failed to point out any error in the Examiner's position, we are affirming the § 103(a) rejection with respect to claim 3 and also with respect to claims 13, 16, and 22, which are not separately argued.

DECISION

The rejection of claims 1, 2, 11, 12, 14, 15, 20, and 21 under 35 U.S.C. § 102(b) for anticipation by Eyer is affirmed, as is the rejection of claims 3, 13, 16, and 22 under § 103(a) for obviousness over Eyer in view of Arazi.

16

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. 1.136(a). *See* 37 C.F.R. §§ 41.50(f) and 41.52(b).

<u>AFFIRMED</u>

KIS

INTEL CORPORATION
c/o INTELLEVATE, LLC
P.O. BOX 52050
MINNEAPOLIS, MN 55402